MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

Bundesamt für Sicherheit in der Informationstechnik

Dr. Matthias Peter,
Bundesamt für Sicherheit in der Informationstechnik

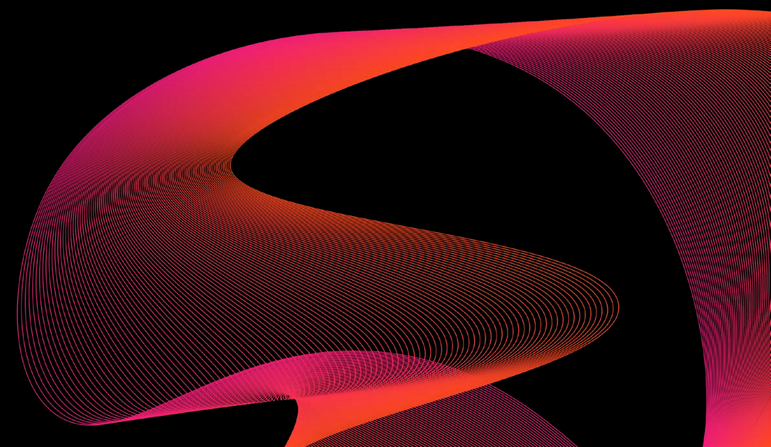
VS Cloud Requirements and Cryptography

MINDSHARE

Bundesamt
für Sicherheit in der
Informationstechnik

Clouds for Classified

- Cloud adoption is inevitable – even in high-security scenarios
- Cloud advantages: scalability, availability, modern IT architecture
- But only selected benefits apply in high-risk environments
- Challenge: Processing classified information regulated by VSA (General Administrative Provision on Material Security)



MINDSHARE

Bundesamt
für Sicherheit in der
Informationstechnik

General Conditions

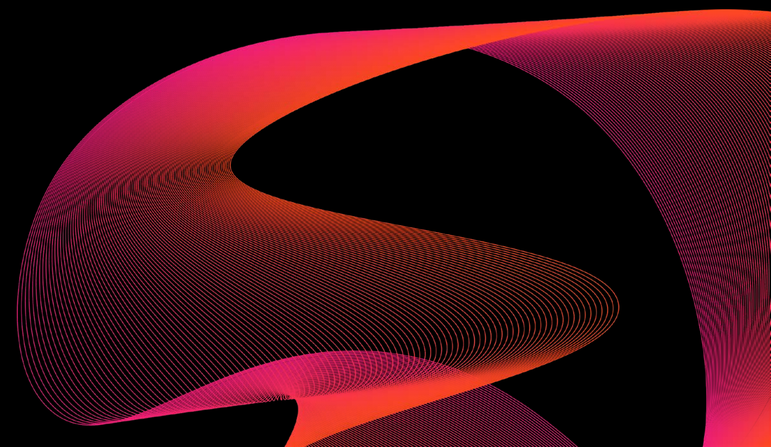
- Cloud architectures handling classified data are VS-IT systems
- Require accreditation under §50 VSA (not §51 product approval)
- Scenario-based assessment is required
- Security Enforcing Services (SES) must be approved under §51 VSA
- Agency head is responsible for accreditation under §50 VSA

MINDSHARE

Bundesamt
für Sicherheit in der
Informationstechnik

Need for Approval Depends on Scenario

- Scenarios: Private, Community, Public
- Access to the Cloud: required in all
- Perimeter protection: required in Private & Community
- Public Cloud: focus on Data at rest, in transit, in use

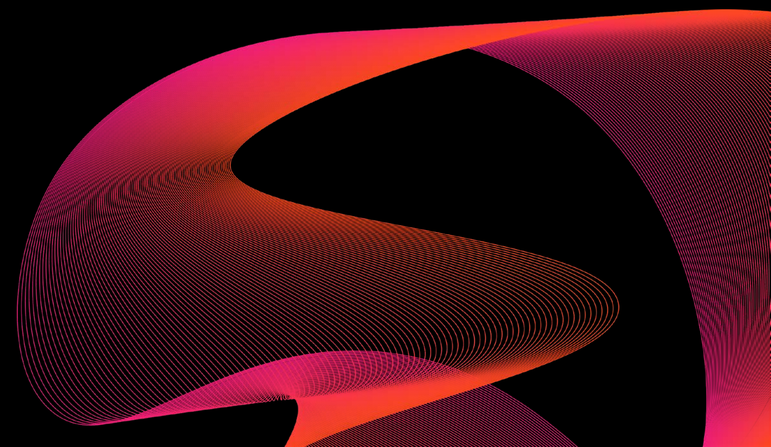


MINDSHARE

Bundesamt
für Sicherheit in der
Informationstechnik

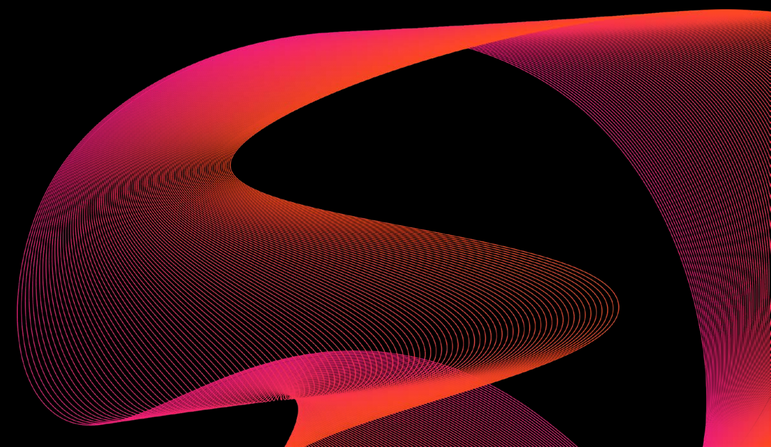
Technical and Cryptographic Evaluation

- Products with security functions (§52 VSA) require approval
- Approval based on BSI approval concept
- Includes CC-like technical evaluation and cryptographic concept (CC: Common Criteria)
- Cryptographic concept covers protocols, primitives, key lifecycle



General Cryptographic Requirements

- Baseline: BSI TR-02102 (crypto algorithms), AIS 20/31 (RNGs)
- Further requirements from CI-Requirements Profiles (VS-APs)
- Example: Long-term secrets stored in dedicated hardware (e.g., to achieve protection against malware and side-channel attacks)

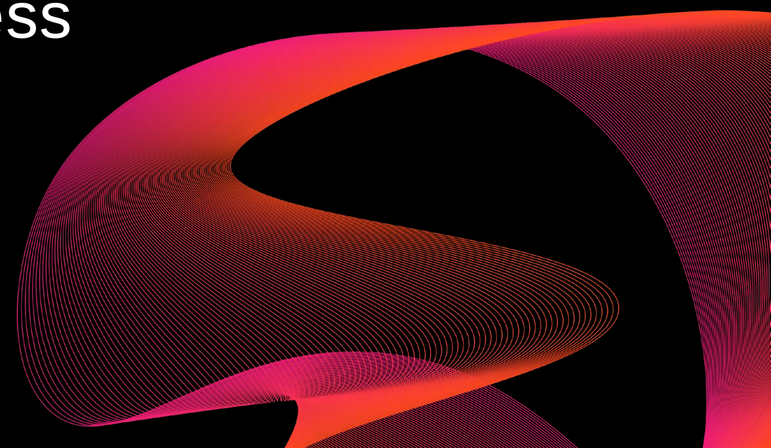


MINDSHARE

Bundesamt
für Sicherheit in der
Informationstechnik

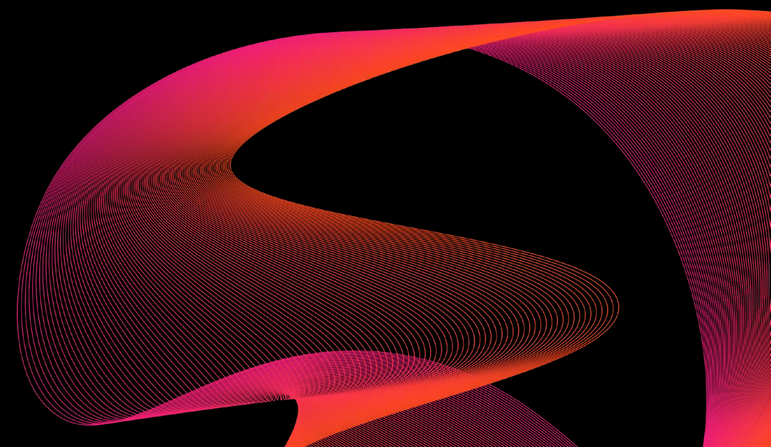
Cloud-Specific Cryptographic Requirements

- Challenges known for a long time (see BSI study from 2015): https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/ZufallinVMS/zufall-in-vms.html
- Lack of smartcard equivalence in virtualized environments
- Workload cloning (keys, identities, RNG states)
- Local RNG: hard to realize without hardware access
- External RNG needs secure channel



Solution Patterns

- No universal templates; depend on scenario and risk
- Goal: portfolio of best practices, not rigid rules (proposals welcome)
- The following approaches may support evaluation, but are not mandatory (nor are they sufficient on its own)

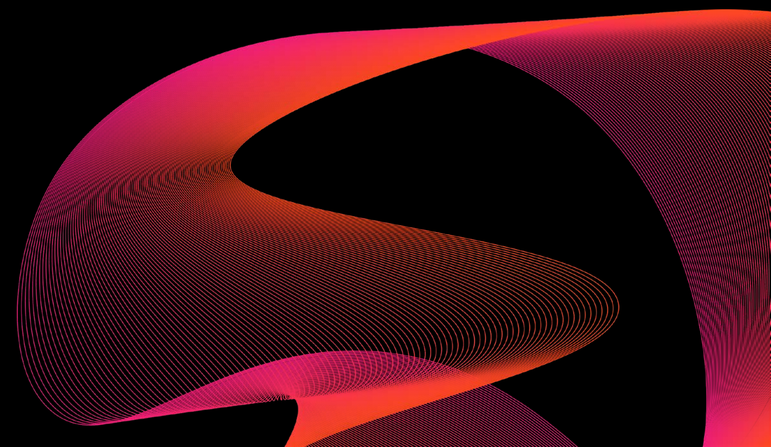


MINDSHARE

Bundesamt
für Sicherheit in der
Informationstechnik

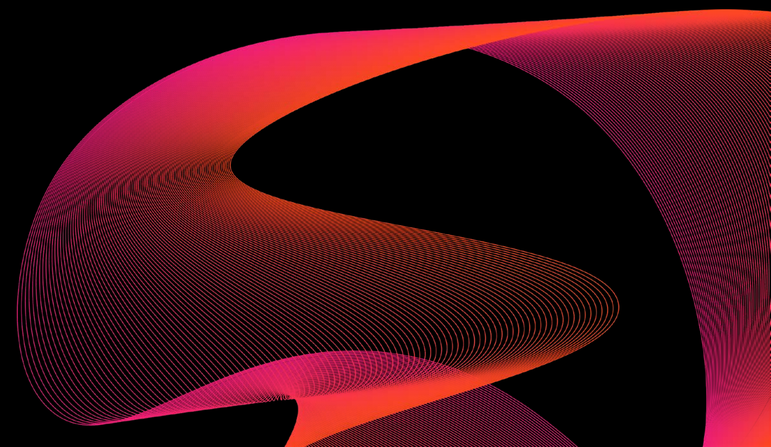
Random Number Generation

- Best: certified RNGs with dedicated noise sources (PTG.3, DRG.4)
- Fallback: NTG.1-compliant software RNG
- Example: Open-source Jitter RNG (towards NTG.1 compliance)



Storing Long-Term Secrets (Example)

- Trustworthy cloud environment required
- Application establishes secure TLS channel to approved HSM
- User authenticates with strong PIN (limited retries)
- HSM performs operations with secret; secret never leaves HSM
- Strong mitigation against malware compromise



MINDSHARE
2025 10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

Bundesamt für Sicherheit in der Informationstechnik

Questions

Dr. Matthias Peter
Bundesamt für Sicherheit in der Informationstechnik
matthias.peter@bsi.bund.de